REMARKS

Applicant has carefully studied the outstanding Office Action. The present amendment is intended to place the application in condition for allowance and is believed to overcome all of the objections and rejections made by the Examiner. Favorable reconsideration and allowance of the application are respectfully requested.

Applicant has amended claims 1, 2 and 4 to more properly claim the present invention, and added new claims 7 - 26. No new matter has been added. Claims 1 – 26 are presented for examination.

In Paragraphs 1 and 2 of the Office Action, claims 1 - 6 have been rejected under 35 U.S.C. §102(e) as being anticipated by Hayes, Jr. et al., U.S. Patent No. 6,339,826 ("Hayes"). In Paragraph 3 of the Office Action, claims 1 – 6 have been rejected under 35 U.S.C. §102(e) as being anticipated by Montague et al., U.S. Patent No. 5,761,669 ("Montague")

Distinctions between Claimed Invention and U.S. Patent No. 6,339,826 to Hayes, Jr. et al. and U.S. Patent No. 5,761,669 to Montague et al.

In one embodiment, the present invention concerns copy protection of digital images stored on a server computer and available for viewing over the Internet. A remote administration tool provides an explorer-type interface for an administrator to set protection status of digital image files. Specifically, as disclosed in the present specification and as illustrated in the user interface of FIG. 13, protection manager 128 (FIG. 1) in remote computer 130 controls protection status of digital image files 108 and 110 resident on server computer 100. Steps 412 – 434 (FIG. 4) disclose computer 130 receiving a site map of folders and files from the file system of computer 100, selecting by a user of computer 130 at least one folder or file, and editing the at least one folder or file's protection status. After setting protection status for selected files, computer 130 sends the protection statuses to server computer 100, which enforces the protection (original specification / page 15, line 18 – page 17, line 10; protection manager 128 of FIG. 1 and the discussion thereof at page 20, lines 7 – 14; FIG. 3 and the discussion thereof at page 22, line 25 – page 24, line 21; FIG. 4 and the discussion thereof at page 24, line 22 – page 27, line 2; user interface illustrated in FIG. 13 and the discussion thereof at page 41, line 16 – page 42, lines 22).

Hayes describes a network computing system in which client terminals download a desktop object and software applications from a central server. The client terminals themselves may have little or no software stored therein, and may even be diskless. With each software application is associated user access permissions that are stored in the central server. When a user logs onto any such client terminal, a user profile is examined to ascertain which applications that user has permission to run. The user's desktop object is configured to only include icons for such applications that the user has permission to run. The client terminal is thus customized for each user when the user logs onto the system.

Additionally, user preference settings for the software applications are also stored on the central server and downloaded to the client terminals. Thus, the software applications run on each client terminal according to the user's preferences. (Hayes / col. 4, line 11 – col. 5, line 26)

In paragraph 5 of the Office Action, the Examiner cites Hayes, FIG. 4 and col. 21, lines 33 – 40, as disclosing displaying a site map of folders and files in a server computer file system. Applicant respectfully submits that FIG. 4 of Hayes shows a listing of individual users. (Hayes, col. 5, lines 46 – 50; col. 9, lines 42 – 52; col. 10, lines 47 and 48) None of the figures of Hayes shows a site map of folders and files.

Montague describes user access control for hardware and software entities on a network, where the network includes a plurality of server computers that run diverse network operating systems such as WINDOWS NT, Novell NETWARE and UNIX. Montague uses generic access control requests for an entity on the network, and translates the request into the specific format required by the network operating system running on the server computer that stores or controls the entity. (Montague / col. 3, lines 37 – 52; col. 7, lines 52 - 65)

In order to further distinguish between the present invention and Hayes and Montague, applicant has amended independent claims 1 and 4 so as to include the limitation of a copy-protection of a file downloaded from the server computer to a client computer, by copy-protection software running on the client computer, if the file is designated as being protected. Neither Hayes nor Montague describe use of protection status for copy-protection of files. Indeed, Hayes and Montague both describe user access control – Hayes describes user access permission for running software applications, and Montague describes user access control to hardware and software entities on a network.

The rejections of claims 1 - 6 in paragraphs 4 and 5 of the Office Action will now be dealt with specifically.

As to amended independent method claim 1, applicant respectfully submits that the limitations in claims 1 of:

"*displaying a site map of folders and files in a server computer file system*", and

"*copy-protecting the at least one file by copy-protection software running on the client computer, if the at least one file is designated by the protection status information as being protected*",

are neither shown nor suggested in Hayes and Montague.

Because claims 2, 3, 13 and 14 depend from claim 1 and include additional features, applicant respectfully submits that claims 2, 3, 11 and 12 are not anticipated or rendered obvious by Hayes, Montague or a combination of Hayes and Montague.

Accordingly claims 1 – 3, 13 and 14 are deemed to be allowable.

As to amended independent system claim 4, applicant respectfully submits that the limitations in claim 4 of:

"*a user interface displaying a site map of folders and files in a server computer file system*", and

"*a copy-protection module residing on a client computer, copy-protecting at least one file downloaded from the server computer to the client computer if the at least one file is designated by the protection status information as being protected*",

are neither shown nor suggested in Hayes and Montague.

Because claims 5, 6, 15 and 16 depend from claim 4 and include additional features, applicant respectfully submits that claims 5, 6, 15 and 16 are not anticipated or rendered obvious by Hayes, Montague or a combination of Hayes and Montague.

Accordingly claims 4 – 6, 15 and 16 are deemed to be allowable.

Regarding new independent claim 7, applicant respectfully submits that the limitations in claim 7 of

"*displaying a site map of folders and files in a server computer file system*", and

"*encrypting at least one file on the server computer, if the at least one file is designated by the protection status information as being protected*",

are neither shown nor suggested in Hayes and Montague.

Because claims 8 and 9 depend from claim 8 and include additional features, applicant respectfully submits that claims 8 and 9 are not anticipated or rendered obvious by Hayes, Montague or a combination of Hayes and Montague.

Accordingly claims 7 - 9 are deemed to be allowable.

Regarding new independent claim 10, applicant respectfully submits that the limitations in claim 10 of

"*a user interface displaying a site map of folders and files in a server computer file system*", and

"*a copy-protection module residing on a client computer, copy-protecting at least one file downloaded from the server computer to the client computer if the at least one file is designated by the protection status information as being protected*",

are neither shown nor suggested in Hayes and Montague.

Because claims 11 and 12 depend from claim 10 and include additional features, applicant respectfully submits that claims 11 and 12 are not anticipated or rendered obvious by Hayes, Montague or a combination of Hayes and Montague.

Accordingly claims 10 - 12 are deemed to be allowable.

<u>Support for New and Amended Claims in Original Specification</u>

Independent claims 1 and 4 have been amended to include the limitation of copy-protection software running on a client computer, for copy-protecting a file downloaded from the server, if the file is designated by the protection status information as being protected. Such copy-protection software is described in the original specification at page 14, line 10 – page 15, line 17, and in the discussion of FIG. 8 at page 35.

New independent claims 7, 11, 15 and 16, and new dependent claims 8 and 12, include the limitation of encrypting files on the server computer that are designated by the protection status information as being protected, and transmitting encrypted files to a client computer instead of unencrypted files. Encryption of files and transmission of encrypted files are described in the original specification at page 13, lines 11 – 13, and in the discussion of element 124 of FIG. 1 and steps 214 – 226 of FIG. 2 at page 18, line 8 – page 19, line 6 and at page 21, lines 3 – 25, respectively.

New dependent claims 9 and 13 include the limitation of decrypting encrypted files that a client computer downloads from the server computer. Decryption of files is described in the original specification at page 13, lines 13 – 22, and in the discussion of element 126 of FIG. 1 and step 228 of FIG. 2 at page 19, lines 7 – 24 and at page 21, line 25 – page 22, line 2, respectively.

New dependent claims 17 and 19 include the limitation of blocking capture of data from a file that is displayed on a computer screen. Such blocking of screen capture is described in the original specification at page 14, line 10 – page 15, line 17 and in the discussion of FIG. 8 at page 35.

New dependent claims 10, 14, 18 and 20 include the limitation of image files. Image files are described throughout the original specification.

New dependent claims 21 and 23 include the limitation of designating all image files within a folder as being protected, in response to user selection of the folder. Such designation is described in the original specification at page 24, lines 6 – 10 and page 42, lines 18 and 19.

New dependent claims 22 and 24 include the limitation of designating all image files referenced within a web page as being protected, in response to user selection of the web page. Such designation is described in the original specification at page 23, lines 27 – page 24, line 5 and page 42, lines 17 and 18.

New independent claims 25 and 26 include the limitation of sending substitute data, in response to a request for data within a file that is designated as being protected. Such substitution of data is described in the original specification at element 124 of FIG. 1 and the discussion thereof at page 18, lines 21 – 25, and at steps 212 – 224 of FIG. 2 and the discussion thereof at page 21, lines 5 – 11.

For the foregoing reasons, applicant respectfully submits that the applicable objections and rejections have been overcome and that the claims are in condition for allowance.

Respectfully submitted,

Dated: October 12, 2004
Squire, Sanders & Dempsey L.L.P.
600 Hansen Way
Palo Alto, CA 94304-1043
Telephone (650) 856-6500
Facsimile (650) 843-8777

By
Marc A. Sockol
Attorney for Applicants
Reg. No. 40,823

CERTIFICATE OF MAILING

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to Mail Stop RCE, the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on
Date: October 12, 2004 By: E. Janikowski
Eileen Janikowski